# Exhibit A

FW_Additional_Information (2)

From: Michele Mair [Michele_Mair@cppoliceservice.com]
Sent: Wednesday, May 11, 2016 4:58 PM
To: Couturier, Paul M. (MP) (FBI)
Subject: FW: Additional Information
Attachments: Incident Response Executive Summary.pdf

Crowdstrike report.

Michele Mair | Special Agent | 1010 Shop Rd St Paul MN 55106

O 651 495 9537 F 651 495 9540| CP Police Service

24/7 Police Control Centre 1 800 716 9132

www.cppoliceservice.com <http://www.cppoliceservice.com/>

From: Tim Winn
Sent: Tuesday, May 10, 2016 10:55 AM
To: Michele Mair
Cc: Ernest Seguin
Subject: RE: Additional Information

Hello Michele,

Please find attached the Crowdstrike report, as requested. The contacts at Crowdstrike are:

Justin Weissert - Director of Proactive Services

412-760-6268

Justin.weissert@crowdstrike.com <mailto:Justin.weissert@crowdstrike.com>

Ryan Jafarkhani- Principal Consultant

Ryan.jafarkhani@crowdstrike.com <mailto:Ryan.jafarkhani@crowdstrike.com>

If there's anything else you need from me in this investigation, please let me know.

Regards,

FW_Additional_Information (2)

Tim

Tim Winn | Director - I&O Project Services | 7550 Ogden Dale Road SE Calgary AB T2C 4X9

O 403 319 4867 | C 403 850 7767 CP

From: Tim Winn
Sent: May 9, 2016 11:41 AM
To: Michele Mair <Michele_Mair@cppoliceservice.com>
Cc: Ernest Seguin <Ernest_Seguin@cpr.ca>
Subject: RE: Additional Information

Hello Michele,

We have received word back from Crowdstrike that we can share the report that they prepared for us regarding Mr. Grupe, as there is a clause in the Master Agreement with them that allows for 3rd party sharing as long as the 3rd party relationship affords the same protection of privacy. Is it fair to assume that CP Police and the Crown Attorney would agree to this?

I am just waiting to get confirmation of the point of contact at Crowdstrike - to address your third request - and then I will send you that and the report.

Regards,
Tim

Tim Winn | Director - I&O Project Services | 7550 Ogden Dale Road SE Calgary AB T2C 4X9

O 403 319 4867 | C 403 850 7767 CP

From: Tim Winn
Sent: May 5, 2016 5:57 PM

To: Michele Mair <Michele_Mair@cppoliceservice.com>
Cc: Ernest Seguin <Ernest_Seguin@cpr.ca>
Subject: RE: Additional Information

Hello Michele,

Per your email below:

1. Attached is Chris Grupe's resignation email.

2. I checked with our Sr. Director for Enterprise Security, Tony Arthur, and he advised me that the Crowdstrike report that he commissioned (following the incident in December) explicitly states that he is not permitted to share the report with any 3rd parties. In light of this, Tony is contacting Crowdstrike to see about getting you a name of a contact there, to see if it is possible to get permission to release the report (and the name of the person who completed it). I hope to have an answer back by tomorrow.

Regards,
Tim

Tim Winn | Director - I&O Project Services | 7550 Ogden Dale Road SE Calgary AB T2C 4X9

O 403 319 4867 | C 403 850 7767 CP

From: Michele Mair
Sent: May 5, 2016 4:41 PM
To: Ernest Seguin <Ernest_Seguin@cpr.ca>; Tim Winn <Tim_Winn@cpr.ca>
Subject: Additional Information

Ernest and Paul-

I am set for a meeting with the State's Attorney next week. They are requesting some additional information regarding GRUPE.

- Copy of resignation email from GRUPE
- Report completed by Crowdstrike
- Contact name for Crowdstrike employee who completed report or

completed the work

Can you forward these to me as soon as possible? Meeting is set for mid-week.

Thanks!

Michele Mair | Special Agent | 1010 Shop Rd St Paul MN 55106

O 651 495 9537 F 651 495 9540| CP Police Service

24/7 Police Control Centre 1 800 716 9132

www.cppoliceservice.com <http://www.cppoliceservice.com/>

------------------------------ IMPORTANT NOTICE - AVIS IMPORTANT ------------------------------ Computer viruses can be transmitted via email. Recipient should check this email and any attachments for the presence of viruses. Sender and sender company accept no liability for any damage caused by any virus transmitted by this email. This email transmission and any accompanying attachments contain confidential information intended only for the use of the individual or entity named above. Any dissemination, distribution, copying or action taken in reliance on the contents of this email by anyone other than the intended recipient is strictly prohibited. If you have received this email in error please immediately delete it and notify sender at the above email address. Le courrier electronique peut etre porteur de virus informatiques. Le destinataire doit donc passer le present courriel et les pieces qui y sont jointes au detecteur de virus. L' expediteur et son employeur declinent toute responsabilite pour les dommages causes par un virus contenu dans le courriel. Le present message et les pieces qui y sont jointes contiennent des renseignements confidentiels destines uniquement a la personne ou a l' organisme nomme ci-dessus. Toute diffusion, distribution, reproduction ou utilisation comme reference du contenu du message par une autre personne que le destinataire est formellement interdite. Si vous avez recu ce courriel par erreur, veuillez le detruire immediatement et en informer l' expediteur a l' adresse ci-dessus. ------------------------------ IMPORTANT NOTICE - AVIS IMPORTANT ------------------------------

CROWDSTRIKE

# Incident Response

CROWDSTRIKE PROFESSIONAL SERVICES

web: WWW.CROWDSTRIKE.COM | [illegible]
email: SERVICES@CROWDSTRIKE.COM

# Canadian Pacific Railway

**Proprietary and Confidential • NOT TO BE SHARED WITH THIRD PARTIES**

This report is provided for situational awareness and network defense purposes only.
DO NOT conduct searches on, communicate with, or engage any individuals, organizations, or network addresses identified in this report. Doing so may put you or your employer at risk and jeopardize ongoing investigation efforts.

Copyright 2014

*YOU DON'T HAVE A MALWARE PROBLEM. YOU HAVE AN* ***ADVERSARY*** *PROBLEM.*

CROWDSTRIKE

# EXECUTIVE SUMMARY

On January 8, 2015 Canadian Pacific Railway ("CPR") engaged CrowdStrike Services, Inc. ("CrowdStrike") to conduct an incident response investigation involving one (1) system in the CPR network. CPR's objective was to determine how the attacker gained access to the environment, if other systems were involved and what information the attacker was targeting.

# BACKGROUND

The initial scope of the compromise involved one (1) Windows system and the unauthorized access of several routers/switches. CPR was alerted to the incident when administrative accounts were being removed on routers/switches in their environment. Falcon Host was leveraged and identified one (1) Windows system and one (1) user account being leveraged by the attacker to SSH and remove administrative accounts from several routers/switches in the CPR environment.

# OBJECTIVES

CrowdStrike's objectives during the course of this engagement were as follows:

- Identify if the initial intrusion was related to an insider threat
- If an insider threat attack occurred, determine the scope of compromise, to include:
    - Initial date of compromise;
    - Initial attack vector;
    - Additional systems compromised/accessed beyond the original scope; and
    - Compromised accounts.
- If an insider threat occurred, assist CPR in providing tactical and strategic remediation recommendations to mitigate the attacker's access as well as future access

# CROWDSTRIKE ANALYSIS

The following is a list of the activities performed by CrowdStrike to accomplish these objectives:

- Conducted kick off meeting with CPR to set goals and expectations for the engagement;
- Triaged one (1) workstation system using Falcon Host; and
- Leveraged router logs provided to CrowdStrike by CPR

CROWDSTRIKE

# KEY FINDINGS

Based on the analysis performed by the CrowdStrike team, the following key findings were noted:

1. The earliest timeframe of attacker activity occurred on 12/17/2015 at 12:01:07 UTC, when the "gru0040" user logged into the 7SCZH12 system.
2. The attacker leveraged "kitty.exe", an SSH utility, and connected to several systems in the CPR environment.
3. The attacker attempted to delete the accounts "cpadmin" and "arcnsparc" from two (2) switches/routers in the CPR environment.
4. The attacker created a new account "admin" and modified its role to be "network-admin" on the switches/routers OGNCORSW02 and OGNCORSW01.

# TIMELINE OF ATTACK

The key attacker activities noted during this investigation are provided in the table at the end of this section. This information has been represented in narrative form below for ease of consumption, but the attack timeline should be referenced for specific details.

- The earliest timeframe of attacker activity occurred on 12/17/2015 at 12:01:07 UTC, when the "gru0040" user logged into the 7SCZH12 system. The attacker logged in interactively at the keyboard of the 7SCZH12 system.
- The attacker used the SSH utility, "kitty.exe", and connected to (15) IP address in the CPR environment starting 12/17/2015 at 12:02:48 UTC.
- CrowdStrike determined that the attacker initiated an SSH connection to 10.190.61.1 on 12/17/2015 at 12:02:48 UTC. Analysis of router logs then show the attacker deleted "cpadmin" and "arcnsparc" accounts on 12/17/2015 at 12:09:29 UTC and 12:09:32 UTC respectively.
- CrowdStrike determined that the attacker initiated an SSH connection to 10.189.248.36 on 12/17/2015 at 12:15:22 UTC. Router logs then show the attacker deleted "arcnsparc" and "cpadmin" accounts on 12/17/2015 at 12:16:57 UTC and 12:17:04 UTC respectively.
- The attacker attempted to SSH to four (4) additional systems in the CPR environment

CROWDSTRIKE

between 12/17/2015 12:19:07 UTC and 12:34:50 UTC respectively.

- Analysis of router logs showed the attacker created the "admin" account with the role "network-admin" on the OGNCORSW02 and OGNCORSW01 switches/routers on 12/27/2015 at 12:40:47 UTC and 12:48:34 UTC.
- The attacker attempted to SSH to six (6) additional systems in the CPR environment between 12/17/2015 12:50:09 UTC and 13:48:00 UTC respectively.

| System Name | Source | Date & Time | Activity Conducted |
|---|---|---|---|
| 7SCZH12 | Falcon Host | 12/17/2015 12:01:07 | Logon type 2: Interactive logon with username "gru0040" onto 7SCZH12 system (this logon is a physical interactive logon at the keyboard) |
| 7SCZH12 | Falcon Host | 12/17/2015 12:02:07 | Ipconfig.exe executed by "gru0040" account |
| 7SCZH12 | Falcon Host | 12/17/2015 12:02:48 | "C:\Program Files\Kitty\kitty.exe" -load "Default Settings" -ssh -P 22 10.190.61.1 |
| N/A | Router Logs | 12/17/2015 12:08:37 | type=start:id=10.188.206.220@pts/1:user=admin:cmd= |
| N/A | Router Logs | 12/17/2015 12:09:29 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=deleted user cpadmin |
| N/A | Router Logs | 12/17/2015 12:09:29 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=deleted v3 user : cpadmin |
| N/A | Router Logs | 12/17/2015 12:09:29 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=configure terminal ; no username cpadmin (SUCCESS) |
| N/A | Router Logs | 12/17/2015 12:09:32 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=deleted user arcnsparc |
| N/A | Router Logs | 12/17/2015 12:09:32 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=deleted v3 user : arcnsparc |
| N/A | Router Logs | 12/17/2015 12:09:32 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=configure terminal ; no username arcnsparc (SUCCESS) |
| N/A | Router Logs | 12/17/2015 12:10:03 | type=start:id=10.188.206.220@pts/1:user=admin:cmd= |
| N/A | Router Logs | 12/17/2015 12:10:03 | type=stop:id=10.188.206.220@pts/1:user=admin:cmd= |
| 7SCZH12 | Falcon Host | 12/17/2015 12:10:13 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=copy running-config tftp:/ (FAILURE) |
| 7SCZH12 | Falcon Host | 12/17/2015 12:11:22 | "C:\Program Files\Kitty\kitty.exe" -load "Default Settings" -ssh -P 22 10.190.248.3 |
| 7SCZH12 | Falcon Host | 12/17/2015 12:12:29 | "C:\Program Files\Kitty\kitty.exe" -load "Default Settings" -ssh -P 22 10.248.248.3 |
| 7SCZH12 | Falcon Host | 12/17/2015 12:12:48 | "C:\Program Files\Kitty\kitty.exe" -load "Default Settings" -ssh -P 22 10.250.248.3 |
| 7SCZH12 | Falcon Host | 12/17/2015 12:13:20 | "C:\Program Files\Kitty\kitty.exe" -load "Default Settings" -ssh -P 22 10.250.248.2 |
| | | 12/17/2015 12:15:07 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc ogndstsw02 (SUCCESS) |
| 7SCZH12 | Falcon Host | 12/17/2015 12:15:22 | "C:\Program Files\Kitty\kitty.exe" -load "Default Settings" -ssh -P 22 10.189.248.36 |
| N/A | Router Logs | 12/17/2015 12:16:34 | type=start:id=10.188.206.220@pts/1:user=admin:cmd= |

CROWDSTRIKE

| System Name | Source | Date & Time | Activity Conducted |
|---|---|---|---|
| **N/A** | Router Logs | 12/17/2015 12:16:57 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=deleted user arcnsparc |
| **N/A** | Router Logs | 12/17/2015 12:16:57 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=deleted v3 user : arcnsparc |
| **N/A** | Router Logs | 12/17/2015 12:16:57 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=configure terminal ; no username arcnsparc (SUCCESS) |
| **N/A** | Router Logs | 12/17/2015 12:17:04 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=deleted user cpadmin |
| **N/A** | Router Logs | 12/17/2015 12:17:04 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=deleted v3 user : cpadmin |
| **N/A** | Router Logs | 12/17/2015 12:17:04 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=configure terminal ; no username cpadmin (SUCCESS) |
| **N/A** | Router Logs | 12/17/2015 12:17:58 | type=start:id=10.188.206.220@pts/1:user=admin:cmd= |
| **N/A** | Router Logs | 12/17/2015 12:17:58 | type=stop:id=10.188.206.220@pts/1:user=admin:cmd= |
| **7SCZH12** | Falcon Host | 12/17/2015 12:19:07 | "C:\Program Files\Kitty\kitty.exe" -load "Default Settings" -ssh -P 22 10.249.248.36 |
| **7SCZH12** | Falcon Host | 12/17/2015 12:19:30 | "C:\Program Files\Kitty\kitty.exe" -load "Default Settings" -ssh -P 22 10.249.248.36 |
| **7SCZH12** | Falcon Host | 12/17/2015 12:22:11 | "C:\Program Files\Kitty\kitty.exe" -load "Default Settings" -ssh -P 22 10.249.248.35 |
| **N/A** | Router Logs | 12/17/2015 12:22:17 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc ogndstsw01 (SUCCESS) |
| **7SCZH12** | Falcon Host | 12/17/2015 12:23:48 | "C:\Program Files (x86)\Notepad++\notepad++.exe" |
| **7SCZH12** | Falcon Host | 12/17/2015 12:33:54 | "C:\Program Files\Kitty\kitty.exe" -load "cppnx7sw01" -ssh -P 22 10.249.248.11 |
| **7SCZH12** | Falcon Host | 12/17/2015 12:34:15 | "C:\Program Files\Kitty\kitty.exe" -load "Default Settings" -ssh -P 22 10.249.248.61 |
| **7SCZH12** | Falcon Host | 12/17/2015 12:34:50 | "C:\Program Files\Kitty\kitty.exe" -load "cppnx7sw01" -ssh -P 22 10.249.248.11 |
| **7SCZH12** | Falcon Host | 12/17/2015 12:35:17 | Ipconfig.exe executed by "gru0040" account |
| **N/A** | Router Logs | 12/17/2015 12:40:42 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc ogncorsw02 (SUCCESS) |
| **N/A** | Router Logs | 12/17/2015 12:40:47 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=added user:admin to the role:network-admin |
| **N/A** | Router Logs | 12/17/2015 12:40:47 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=updated v3 user : admin |
| **N/A** | Router Logs | 12/17/2015 12:40:47 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=configure terminal ; username admin password 0 ******** role vdc-admin (SUCCESS) |
| **N/A** | Router Logs | 12/17/2015 12:41:37 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc ogncorsw01 (SUCCESS) |
| **N/A** | Router Logs | 12/17/2015 12:42:05 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc ogncorsw02 (SUCCESS) |
| **N/A** | Router Logs | 12/17/2015 12:42:23 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc ogndstsw02 (SUCCESS) |
| **N/A** | Router Logs | 12/17/2015 12:44:57 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=dir bootflash:/ (SUCCESS) |
| **N/A** | Router Logs | 12/17/2015 12:45:09 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc ogncorsw01 (SUCCESS) |
| **N/A** | Router Logs | 12/17/2015 12:45:38 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=dir bootflash:/vdc_2/ (SUCCESS) |
| **N/A** | Router Logs | 12/17/2015 12:46:00 | type=stop:id=10.188.206.220@pts/1:user=admin:cmd=shell terminated gracefully |
| **N/A** | Router Logs | 12/17/2015 12:48:21 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc ogncorsw01 (SUCCESS) |
| **N/A** | Router Logs | 12/17/2015 12:48:34 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=added user:admin to the role:network-admin |

CROWDSTRIKE

| System Name | Source | Date & Time | Activity Conducted |
|---|---|---|---|
| N/A | Router Logs | 12/17/2015 12:48:34 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=updated v3 user : admin |
| N/A | Router Logs | 12/17/2015 12:48:34 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=configure terminal ; username admin password 0 ******** role vdc-admin (SUCCESS |
| 7SCZH12 | Falcon Host | 12/17/2015 12:50:09 | "C:\Program Files\Kitty\kitty.exe" -load "Default Settings" -ssh -P 22 10.249.248.36 |
| 7SCZH12 | Falcon Host | 12/17/2015 12:50:14 | "C:\Program Files\Kitty\kitty.exe" -load "cppnx7sw02" -ssh -P 22 10.249.248.12 |
| N/A | Router Logs | 12/17/2015 12:50:42 | type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc ogndstsw01 (SUCCESS) |
| N/A | Router Logs | 12/17/2015 12:51:33 | 2015:type=stop:id=10.188.206.220@pts/1:user=admin:cmd=shell terminated gracefully |
| 7SCZH12 | Falcon Host | 12/17/2015 13:15:44 | "C:\Program Files\Kitty\kitty.exe" -load "Default Settings" -ssh -P 22 10.249.248.113 |
| 7SCZH12 | Falcon Host | 12/17/2015 13:16:24 | "C:\Program Files\Kitty\kitty.exe" -load "ognnx7sw01" -ssh -P 22 10.189.248.11 |
| 7SCZH12 | Falcon Host | 12/17/2015 13:16:26 | "C:\Program Files\Kitty\kitty.exe" -load "ognnx7sw02" -ssh -P 22 10.189.248.12 |
| 7SCZH12 | Falcon Host | 12/17/2015 13:48:00 | "C:\Program Files\Kitty\kitty.exe" -load "Default Settings" -ssh -P 22 10.189.52.2 |

# REMEDIATION RECOMMENDATIONS

Given the scope of this engagement, CrowdStrike did not specifically discuss the breadth of security controls employed by CPR to protect its environment. However, CrowdStrike believes the following best practice recommendations may be relevant to the organization based on high-level observations and discussions with management. These recommendations should be vetted with the appropriate groups prior to implementation and considered alongside alternative security objectives on the security roadmap. CrowdStrike is available to assist CPR in determining an appropriate security prioritization as needed.

## 1. Central Logging

Centralized logging would allow all logs on the network to be sent to a central repository for preservation. If there is ever a system compromise, this centralized log server would contain all the forensic evidence.

## 2. Time Synchronization of Logging

CrowdStrike recommends synchronizing timestamps for all central log sources into one time zone, preferably GMT time. This will aid an investigator to follow a unified timeline if an attack were to occur in the future.

## 3. Terminated Employee Access

When terminating an employee, especially an employee with administrative privileges in the network environment, CrowdStrike recommends all company assets the employee has in possession be immediately seized and all access revoked.

## CONCLUSION

CrowdStrike determined that the attacker physically logged into the 7SCZH12 system to initiate SSH connections to victim systems, including routers/switches, in the CPR environment. This would require the attacker to have substantial knowledge of the environment, administrative privileges and to have been physically at the keyboard on the 7SCZH12 system during the time of the attack. The attacker attempted to remove privileged accounts from the routers/switches and to create a new privileged account on the routers/switches.